Mobile Switching Center Database

Table of Contents

Mobile Switching Center Database..... 2

Network Authentication (GSM) -1..... 8

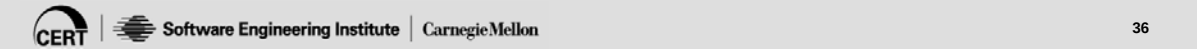
Mobile Switching Center Database..... 9

Notices..... 11

Mobile Switching Center Database

The MSC database contains critical subscription data about each network user.

- HLR (Home Location Register)
- VLR (Visitor Location Register)
- AUC (Authentication Center)
- EIR (Equipment Identity Register)



**036 Then you have the Mobile Switching Center database. There are a lot of databases associated with this. However these are the four primary databases we'll look at: the Home Location Register; the Visitor Location Register; the Authentication Center; and the Equipment Identity Register.

The Home Location Register stores-- and we'll get into these acronyms later-- the IMSI and the MSISDN on a GSM call.

The IMSI is the International Mobile Subscriber Identity. It is the number associated with a SIM card. So each SIM card that's purchased has a

specific IMSI associated with it. You're never supposed to see a duplicate IMSI on the network. If you do, that means somebody's probably changed the digital number in their SIM card and is pretending to be somebody they're not actually. So they're trying to make free phone calls or whatever.

There should be one IMSI-- each IMSI should be unique, let's put it that way. There shouldn't be duplicate IMSIs.

MSISDN, Mobile Subscriber ISDN Number-- and that's the way it's actually written in the 3GPP standard; I don't know why they don't detail what ISDN means-- is the phone number you dial to reach a subscriber.

So I call 210-555-5555. That is the person's MSISDN, if they're on a GSM network. CDMA networks have the same sort of numbers, or identifiers; they're just named differently. So on a CDMA network, the MSISDN is the MDN-- which is the Mobile Directory Number-- and the IMSI is sort of encapsulated in the ESN, the Electronic Serial Number, or the MEID, depending on how old the phone is; Mobile Equipment Identity.

The HLR is the primary database that the phone company uses. It has all your subscriber information. It has the address associated with the SIM card. When you purchase a SIM card in the U.S., you have to provide them an address to associate that SIM card with.

The VLR is the Visitor Location Register. It is used when you're roaming on a tower. Now this is not what we normally consider roaming. When I normally say roaming, I think I'm an AT&T customer but I'm in an area that doesn't have AT&T service. So I'm roaming on T-Mobile's network.

When we talk about roaming with the VLR, you're considered roaming to whatever cell tower you're connected to. And it has a lot of the same information that the HLR has. It has your IMSI; it has the Ki, which is the encryption key you use to actually communicate. It has the MSISDN.

However, once you disconnect from a VLR, depending on the network you're a part of, it is supposed to purge your information from the database within a certain length of time.

I can't tell you how long AT&T's is, or T-Mobile's is, but it's not a very long time. But before it's purged, all that information is copied up to the HLR. So the HLR contains a master database of what cell towers you've been connected to, your call history, your call logs and all that information.

The AUC, the Authentication Center, is what allows your phone on the network in the first place. So when I first turn on-- if I turn off my phone every day and I turn it on in the morning, when I first turn my phone on, my phone connects to the

network and the Authentication Center goes: Is this phone allowed on the network, yes or no?

It checks the IMSI, or is supposed to check the IMSI to make sure it's valid. It's supposed to check the Equipment Identity Register to make sure the phone isn't on the EIR. And if that's true, it says: Okay, you can connect to the- to our network.

The AUC and the SIM card contain the encryption algorithm that's going to be used for the communication. Between the Ki and the-- the Ki and IMSI are used as part of the encryption process. So the Ki is never transmitted. Yes sir?

Student: With CDMA, is that private key hard-coded into the device?

Shawn Fleury: Yes. It's not coded on the- it's not coded on the SIM card since CDMA phones don't have a SIM card. It's hard-coded to the phone itself.

Student: Okay.

Shawn Fleury: So it says: Okay, we know the phone has this Ki. So we're going to use this Ki, plus the phone's IMSI, to encrypt the conversation.

It goes a step beyond that though. They don't want the IMSI constantly sent in the clear, because that's-- that describes the SIM card itself. And if somebody gets the IMSI, they could then pretend to be you;

because there's a weakness in the Ki, the algorithm that's used. So I can actually break the encryption, if I can get the IMSI.

So what happens is the first time you connect, you're given a temporary IMSI or a TMSI. And your TMSI, depending on the network, switches every so often. The AUC and the phone agree: This is going to be how the TMSI changes and this is what it's going to change to, and this is when we're going to change. And then it will change every so often.

Now the problem is, with the way it's implemented, it's not every minute necessarily, it's not every two minutes. It could be like five or ten minutes.

There's actually an attack that was discovered where if I have my phone- if I have a phone and I have it connected to a laptop and I have special software on the laptop, I can call another mobile device and find out what the current TMSI is. It doesn't allow me to listen in on the conversations. What it does allow me to do is determine which cell tower that user is connected to.

So if I'm a robber and I want to rob Brian's house. I call the phone, let it dial once. It might not even dial on his side, so he never sees there's an incoming call; because I hang up as soon as there's one dial. I then check the software to see which tower he was last connected to; and I can say, "Oh I know he's not at

home." I can now go rob the house because I know he's not going to be there.

So that's the weakness with the way the TMSI was implemented. But it is what it is.

And then we have the Equipment Identity Register. When a phone is stolen, or when it's not behaving nicely on the network; so it's something broken in it, so it's always transmitting, let's say.

I call AT&T and I say, "My phone was stolen" or "My phone isn't quite working right. I don't understand it." They say, "Okay, come in, we're going to-- you're going to have to get a new phone." Blah-blah-blah-blah.

And then they add, or they're supposed to add, my current phone's IMEI-- which is the International Mobile Equipment Identity; it's basically the serial number for the handset-- to the Equipment Identity Register. And that prevents, or is supposed to prevent, that phone from ever connecting to any network. The EIR is supposed to be shared with all cellular providers around the world. Supposed to be; it's not necessarily done.

So if I have a phone stolen here and the phone is sent to Mexico, more than likely the telephone companies in Mexico aren't checking the EIR. So they're not preventing that phone from being on the network.

So the database is there. For the most part the U.S. companies normally use it. But it's not 100 percent. But the real purpose of it is to prevent stolen equipment from being used on the network. Yes?

Network Authentication (GSM) -1

Network Authentication (GSM) -1

Mobile devices following the GSM standard require valid data from the unit and SIM (Subscriber Identity Module).

- IMEI (International Mobile Equipment Identifier)
- IMSI (International Mobile Subscriber Identity)
- TMSI (Temporary Mobile Subscriber Identity)
- MSISDN (Mobile Station International Subscriber Directory Number)
- Ki (Authentication Key)

IMEI from mobile devices is checked against the provider's EIR.

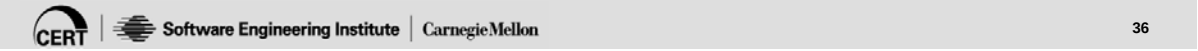
- Units are rejected from the network if stolen or blacklisted.

**037 Student: Now what happens if the network sees two-- think of the guys in the '80s that were doing cell phone hacking. Weren't they just randomly generating ESNs or something like that? What happens if the network sees two duplicate ESNs sitting on there? Does it do anything?

Mobile Switching Center Database

The MSC database contains critical subscription data about each network user.

- HLR (Home Location Register)
- VLR (Visitor Location Register)
- AUC (Authentication Center)
- EIR (Equipment Identity Register)



**036 Shawn Fleury: So in the '80s the problem was the full analog thing. I could actually see in clear text the ESN and the MDN rolling across the network. Take those numbers, put them on a new phone, clone it on to a phone, and then use that phone to make the phone call.

For current phones, your ESN, MDN or IMSI, IMEI, should only appear once on a particular network. So if AT&T sees duplicate IMEIs, I'm going to say more than likely-- because I haven't gone to them and asked-- more than likely they're going to cut off all of them until the subscriber goes to them and goes, "Why did you

cut my service?" And then they'll reinitialize that one. Same with CDMA for Verizon or Sprint.

They're digital numbers. I can change them in my phone. IMEIs, which is the handset identifier, I doubt most telephone companies are doing checks for duplicate IMEIs. They're much more concerned about billing you in the first place. Because the handset identifier, yes it's used to confirm who you are. But they really care about the IMSI on the SIM card.

So if they see duplicate IMSIs, they're going to have an issue. If they see duplicate handset IDs, some companies may cut it off some companies don't care.

But you're right, it is a unique value. There's stuff they could do. But I don't think a lot of them are doing anything with that information; unless it's they're trying- somebody's doing billing fraud or something along those lines.

Notices

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.